СИСТЕМА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННОЙ ОРГАНИЗАЦИИ

Видяйкина Татьяна Сергеевна *
Студент
epifankat@yandex.ru

*ФГБОУ ВО «Мордовский государственный университет им. Н. П. Огарёва»,
г. Саранск, Россия

Аннотация:
В статье представлена система менеджмента информационной безопасности, благодаря которой современная организация дает гарантии защищенности не только всего потока информации, но и её активов. Рассмотрены цель и основные задачи Стандарта ISO/IEC 27001, а также основные показатели для формирования комплексных требований к безопасности информации. Выделены преимущества и возможные проблемы при внедрении Стандарта.

Ключевые слова:
система менеджмента качества, информационная безопасность (ИБ), система менеджмента информационной безопасности (СМИБ), ISO/IEC 27001, защита активов организации, оценка рисков

УДК 338.45

Для цитирования: **Видяйкина Т.С.** Система менеджмента информационной безопасности в современной организации / Т.С. Видяйкина // Контентус. – 2023. – № 7S. – Т.3. – С. 4 – 10.

На сегодняшний день можно с уверенностью сказать, что системы менеджмента качества и информационной безопасности являются неразрывными. Нельзя представить современный мир без высокотехнологичных средств, число и качество которых становится все больше и лучше, что позволяет предприятиям повысить свою конкурентоспособность. Но наряду с этим вырастают и риски. Именно поэтому возникает необходимость в информационной безопасности (ИБ).

Крупнейшие организации достаточно быстрыми темпами внедряют систему информационной безопасности. Под информационной безопасностью принято понимать сохранение и защиту информационных ресурсов, систем и оборудования, предназначенных для использования, сбережения и передачи этой информации. Определяющими факторами для этого являются различные угрозы и риски. Но прежде чем это определить, нужно дать соответствующую оценку всем бизнес-процессам конкретного предприятия. Помимо этого, четкая оценка будет

способствовать не просто повышению качества, конкурентоспособности и повышение прибыли, но и позволит в трудных ситуациях выстроить план непрерывной работоспособности организации и ее членов. Именно поэтому основной целью системы менеджмента информационной безопасности является минимизация всевозможных рисков и повышение защита ИБ.

Система менеджмента информационной безопасности (СМИБ) – часть общей системы управления, основанной на подходе бизнес-рисков, с целью создать, внедрить, эксплуатировать, постоянно контролировать, анализировать, поддерживать в рабочем состоянии и улучшать информационную безопасность [1].

В данную систему входит персонал, производимые процессы и ИТ-системы, объединенные путем внедрения процессов риск-менеджмента.

ISO/IEC 27001 (ГОСТ Р ИСО/МЭК 27001) – это международный Стандарт по информационной безопасности, включающий требования по ИБ для создания и развития СМИБ [10].

Данный Стандарт направлен на сбережение компании её активов и обеспечение целостности, надежности и конфиденциальности информации. Основополагающим пунктом для внедрения ISO/IEC 27001 является определение активов, в роли которых могут выступать не только ИТ-процессы, но и оборудование, инфраструктура, человеческие ресурсы и т.д. То есть активом является вся информация, включая методы и средства ее обработки, которая представляет ценность для организации [7].

Именно поэтому основной целью данного Стандарта является оценка ИБ предприятия и выбор наиболее подходящих мер по управлению безопасностью и защите активов предприятия и предоставление соответствующих гарантий для заинтересованных сторон.

Основные задачи Стандарта [3]:

- установление единых требований по обеспечению ИБ организации;

- обеспечение взаимодействия руководства и сотрудников организации;

- повышение эффективности мероприятий по обеспечению и поддержанию ИБ организации.

С целью формирования комплексных требований к безопасности информации Стандарт определяет 3 основных показателя:

- оценка рисков, с которыми сталкивается организация (определение угрозы для ресурсов, их уязвимость и вероятность возникновения угроз, а также возможный ущерб);

- соблюдение законодательных, нормативных и договорных требований, которые должны выполняться самой организацией, ее партнерами по бизнесу, подрядчиками и поставщиками услуг;

- формирование комплекса принципов, целей и требований к обработке информации, разработанных организацией для поддержки своей деятельности.

ISO/IEC 27001 (ГОСТ Р ИСО/МЭК 27001) в организациях используется как модель для разработки и внедрения наиболее подходящей СМИБ с целью достижения поставленных задач и эффективной работы всех бизнес-процессов. СМИБ включает в себя организацию деятельности, управление рисками и меры по защите информации, то есть все то, что позволяет обеспечить информационную безопасность предприятия. Немаловажным аспектом ISO/IEC 27001 является то, что данный Стандарт согласован с другими стандартами и служит их дополнением [5, с. 50].

Так, современные предприятия уже пользуются интегрированной системой менеджмента при интегрировании Стандартов ISO/IEC 27001 и ISO 9001 (Менеджмент качества). При объединении данных стандартов организация сможет не только повысить качество продукции со всеми гарантиями ее защищенности, но и повысить свою конкурентоспособность. Помимо ISO 9001, Стандарт ISO/IEC 27001 может быть интегрирован со Стандартами ISO 14000 (Менеджмент окружающей среды), ISO 20000 (Управление ИТ-услугами), ISO 45000 (Охрана труда и техника безопасности), ISO 31000 (Менеджмент рисков) и другими.

Существует 10 основных этапов построения системы менеджмента информационной безопасности [2, 11]:

Этап 1.	• Подготовка планов мероприятий. На данном этапе эксперты осуществляют сбор организационно-распорядительных документов (ОРД) и других рабочих материалов, связанных с созданием СМИБ и информационных систем компании, планируемых к использованию механизмов и средств обеспечения ИБ. Кроме того, составляется план мероприятий, который согласуется и утверждается с руководством компании.
Этап 2.	• Проверка на соответствие ISO/IEC 27001. Анкетирование и интервьюирование менеджеров и сотрудников подразделений. Анализ СМИБ компании на соответствие требованиям стандарта ISO/IEC 27001.
Этап 3.	• Анализ нормативно-правовых и организационных документов, основанных на организационной структуре компании. По его результатам определяется область защиты и разрабатывается эскиз политики ИБ компании.
Этап 4.	• Анализ и оценка рисков ИБ. Разработка методики по управлению рисками компании, а также их анализ. Анализ информационных ресурсов компании для выявления угроз защищаемых активов. Проведение консультаций для специалистов компании. Сопоставление фактического и необходимого уровня безопасности и его оценка. Расчет рисков и уязвимостей для каждого актива. Ранжирование рисков и выбор комплексов мероприятий по их снижению. Примерный расчет эффективности внедрения [6].
Этап 5.	• Разработка и реализация планов мероприятий по ИБ. Разработка положения в соответствии с ISO/IEC 27001. Разработка плана учета и устранения рисков. Подготовка отчетов для руководителя компании.
Этап 6.	• Разработка нормативных и ОРД. Разработка и утверждение окончательной Политики ИБ и соответствующих ей положений. Разработка стандартов, процедур и инструкций, обеспечивающих нормальное функционирование и эксплуатацию СМИБ компании.
Этап 7.	• Внедрение комплексных мероприятий по снижению рисков ИБ. Проведение оценочных мероприятий и контроль по эффективности снижения рисков в соответствии с утвержденным руководством планом работ по устранению рисков.
Этап 8.	• Обучение персонала. Разработка планов мероприятий и внедрение программ по обучению и повышению квалификации сотрудников компании с целью эффективного донесения принципов ИБ до всех сотрудников, особенно тех, кто работает с ключевыми бизнес-процессами.
Этап 9.	• Систематизация и формирование отчетности. Представление результатов по выполнению работ руководству компании. Подготовка документов к лицензированию на соответствие ISO/IEC 27001 и передача их в сертифицирующую организацию.
Этап 10.	• Анализ и оценка результатов внедрения СМИБ. Разработка рекомендаций по совершенствованию ИБ.

Можно выделить некоторые преимущества внедрения в компанию СМИБ [4, 8-9]:

– повышение устойчивости компании к воздействию внешних факторов, связанных с ИБ;

– снижение рисков, предотвращение и снижение ущерба от инцидентов ИБ;

– защищенность, конфиденциальность и целостность всех данных;

– быстрое и своевременное реагирование на возникшие риски и угрозы;

– эффективное использование ресурсов;

– повышение доверия клиентов, партнеров и других заинтересованных сторон;

– снижение уровня затрат, связанных с ИБ, оценкой рисков и СМИБ;

– укрепление имиджа компании, выход на международный уровень;

– прозрачность управления, повышение стабильности функционирования организации и др.

Несмотря на большой перечень всех преимуществ, могут возникнуть проблемы, которые затруднят внедрение СМИБ:

– неполное или неправильное определение целей и задач для внедрения СМИБ;

– необоснованный подход к выбору программных продуктов и обеспечений, а также разработка соответствующая разработка требований по их использованию;

– экономические затраты на ИБ и связанное с ней оборудование;

– слабая степень подготовки и недостаточная компетентность персонала и руководства, связанная с ИБ и СМИБ;

– привлечение сторонних организаций и специалистов, которые помогут организации привести бизнес-процессы в соответствие со всеми требованиями [4].

Таким образом, на сегодняшний день СМИБ является неотъемлемой частью любой организации. Она базируется на конфиденциальности, целостности и доступности информации и требует ответственного подхода не только со стороны руководителя, но и со стороны сотрудников, что способствует повышению качества и надежности оказываемых услуг. ISO/IEC 27001 (ГОСТ Р ИСО/МЭК 27001) обеспечивает управление всеми потоками информации в организации, их корректное использование, предотвращение искажения и утечки информации, а также минимизирует риски и потери при кибератаках. СМИБ позволит предприятию сохранить свой имидж, повысить безопасность и доверие со стороны заинтересованных сторон и дать им гарантии защищенности.

Список использованных источников

1. «Система менеджмента информационной безопасности» википедия. URL: https://ru.wikipedia.org/wiki/Система_менеджмента_информационной_безопасности

2. **Шахалов И.Ю., Райкова Н.О.** К вопросу об интегрировании систем менеджмента качества и информационной безопасности. // Правовая информатика. 2014. № 2. С. 20-25.

3. Система менеджмента информационной безопасности ISO 27001 [Электронный ресурс]. – БелПроектКонсалтинг. - URL: https://bpk.by/iso-27001?ysclid=lg2brn2ba2350674735

4. Система защиты информации: преимущества и особенности внедрения [Электронный ресурс]. – Стандарт качества. - URL: https://standartno.by/blog/articles/management-system/information-security-iso-27001/sistema-zashchity-informatsii-preimushchestva-i-osobennosti-vnedreniya/

5. **Райкова Н.О.** Об интеграции систем менеджменте информационной безопасности и качества. // Вопросы кибербезопасности. 2013. № 3. С. 47-53.

6. **Марков А.С., Цирлов В.Л.** Управление рисками – нормативный вакуум информационной безопасности. // Открытые системы. СУБД. 2007. № 8. С. 63-67.

7. **Шпер В.Л.** О стандарте ISO/IEC 27001. // Методы менеджмента качества. 2008. № 3. С. 60-62.

8. Менеджмент информационной безопасности [Электронный ресурс]. – СёрчИнформ. - URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/dokumenty-po-informatsionnoj-bezopasnosti/instruktsii-po-informatsionnoj-bezopasnosti/sluzhba-informatsionnoj-bezopasnosti/menedzhment-informatsionnoj-bezopasnosti/?ysclid=lg24g5nw63231842846

9. **Чесалов А.** Методология внедрения ISO/IEC 27001:2005 при построении СУИБ. // PC Week/RE. 2007. №3 (561). URL: https://www.itweek.ru/infrastructure/article/detail.php?ID=81938

10. **Маццоли Р., Джахиу Д., Кросс К., Вукос-Уокер К., Бак А., Строум Д., Войтасен Д.** Стандарты управления информационной безопасностью ISO/IEC 27001:2013. // Microsoft. 2023. URL: https://learn.microsoft.com/ru-ru/compliance/regulatory/offering-iso-27001

11. **Шахалов И.Ю., Дорофеев А.В.** Основы управления информационной безопасностью современной организации. // Правовая информатика. 2013. № 3. С. 4-10.

INFORMATION SECURITY MANAGEMENT SYSTEM IN A MODERN ORGANIZATION

Vidyaikina Tatiana Sergeevna**
Student
epifankat@yandex.ru

**National Research Mordovia State University,
Saransk, Russia

Abstract:
The article presents an information security management system, thanks to which a modern organization can guarantee the security of not only the entire flow of information, but also its assets. The purpose and main objectives of the ISO/IEC 27001 Standard are considered, as well as the main indicators for the formation of complex information security requirements. The advantages and possible problems in the implementation of the Standard are highlighted.

Keywords:
quality management system, information security (IS), information security management system (ISMS), ISO/IEC 27001, protection of the organization's assets, risk assessment